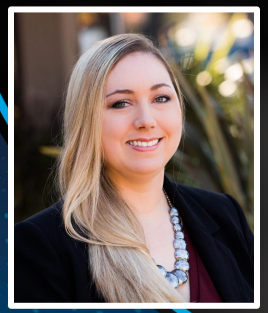
CJIS Security Policy Version 5.9.2 CJISD-ITS-DOC-08140-5.9.2 Brief



Lindsey Shaw
2023

MOTOROLA SOLUTIONS

TIMELINE OF A CYBER EVENT

What Happens During a Cyber Breach

Initial Access
OCT 04, 2022 (Tue 2:12 PM)
ACCESS CREDENTIALS STOLEN

Privilege Escalation
OCT 05, 2022 (Wed 3:23 AM)
GAINING THE RIGHT PERMISSIONS

Lateral Movement
OCT 07, 2022 (Fri 11:34 PM)
TARGET NETWORK ACCESSED

Execution
OCT 08, 2022 (Sat 5:04 PM)
PAYLOAD (RANSOMWARE)

System Down
OCT 08, 2022 (Sat 8:43 PM)
COMPLETE SYSTEM FAILURE

Loss of Service
OCT 13, 2022 (Thur 4:03 AM)
9-1-1 SYSTEM DOWN FOR 4 DAYS

CHANGES IN POLICY - 5.9.2

POLICY CHANGES FROM 5.9.1 -> 5.9.2

Added Sections 5.14 and 5.15

3. **Section 5.14 System and Services Acquisition, Spring 2022, APB#11, Fast Track #1, Unsupported System Components in the *CJISSECPOL***: update the CJIS Security Policy requirements for ***Unsupported System Components***.
4. **Section 5.15 System and Information Integrity, Spring 2022, APB#10, SA#5, Modernization System and Information Integrity (SI) in the *CJISSECPOL***: modernize the CJIS Security Policy requirements for ***System and Information Integrity Policy and Procedures, Flaw Remediation, Malicious Code Protection, System Monitoring, Security Alerts, Advisories, and Directives, Software, Firmware, and Information Integrity, Spam Protection, Information Input Validation, Error Handling, Information Management and Retention, Memory Protection***.

SCOPE & DATA SETS

SCOPE

"CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information.

The CJIS Security Policy provides minimum security requirements associated with the creation, VIEWING, modification, TRANSMISSION, DISSEMINATION, STORAGE, or destruction of CJI."

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

SYSTEMS AFFECTED

“Equipment used to establish said connection.”

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- Information and Data: Both terms refer to CJI.
- System, Information System, Service, or named applications like NCIC: all refer to connections to the FBI’s criminal justice information repositories and the equipment used to establish said connections.

FBI CJIS DATA SETS

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

+ Criminal History Record Information (CHRI) (Pg 10)

MINIMUM STANDARDS

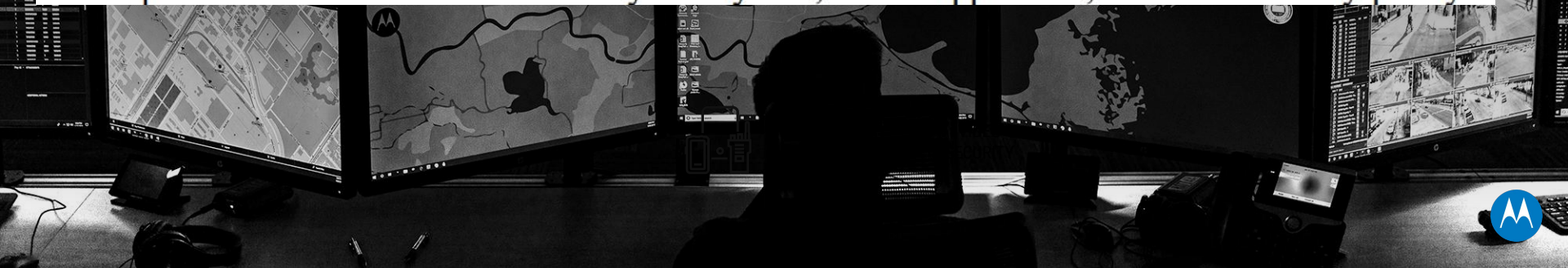
RELATIONSHIP TO LOCAL SECURITY POLICIES

CJIS IS THE MINIMUM STANDARD

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy.



NON-COMPLIANCE PENALTIES

What happens if an agency is non-compliant with 5.9.2?

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

---

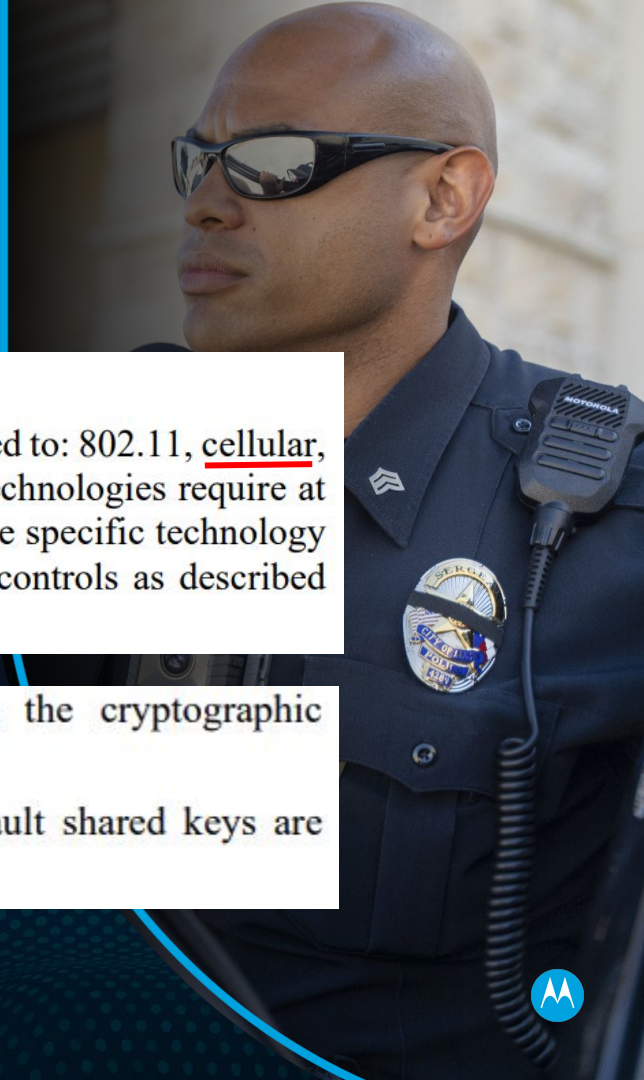
[5] This requirement is sanctionable for audit beginning October 1, 2023.

Sections 5.14 and 5.15 are sanctionable for audit Oct. 1, 2023.

LEGACY SECTIONS 5.13 & 5.10 (OLD CJIS 5.9.1 POLICY)

POLICY FOR WIRELESS DEVICES

Including Radio & LTE



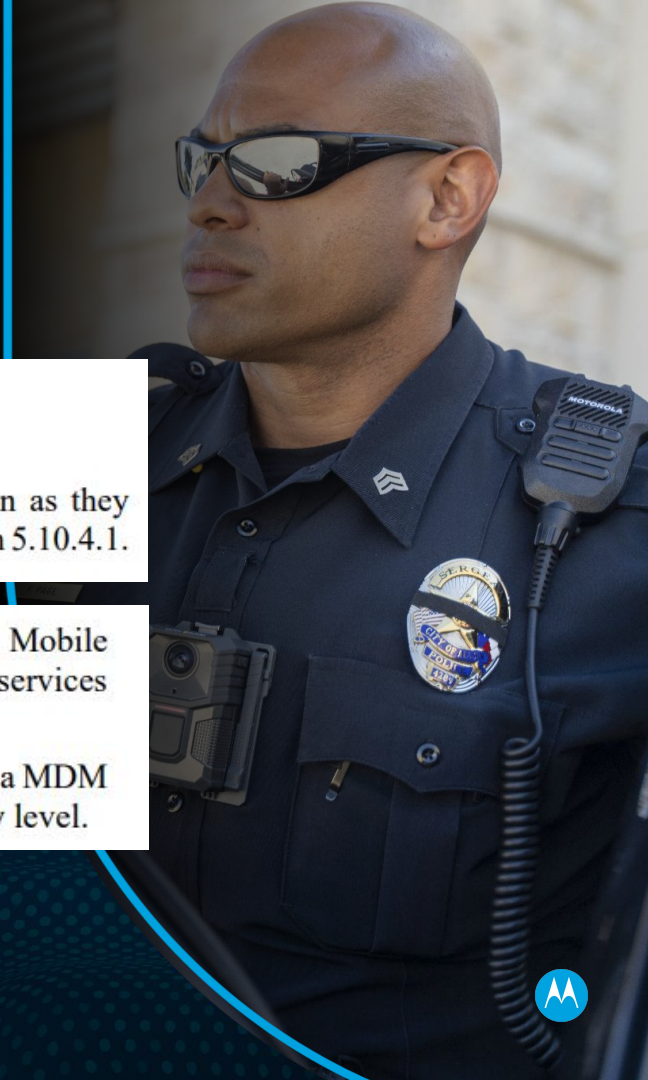
5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.

POLICY FOR WIRELESS DEVICES

Including Radio & LTE



5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

POLICY FOR WIRELESS DEVICES

Including Radio & LTE

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third-party MDM, application, or supporting service infrastructure.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.

SECTION 5.14

[5] This requirement is sanctionable for audit beginning October 1, 2023.

SECTION 5.14

No Unsupported Systems; Must Have Maintenance Contracts

5.14 SYSTEM AND SERVICES ACQUISITION (SA)

SA-22 UNSUPPORTED SYSTEM COMPONENTS[5]

Control:

a. *Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or*
b. *Provide the following options for alternative sources for continued support for unsupported components: original manufacturer support, or original contracted vendor support.*

Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components

SECTION 5.15

SECTION 5.15

SI-1

5.15 SYSTEM AND INFORMATION INTEGRITY (SI)

SI-1 POLICY AND PROCEDURES[6]

Control:

a. *Develop, document, and disseminate to all organizational personnel with system and information integrity responsibilities and information system owners:*

   1. *Agency-level system and information integrity policy that:*

      (a) *Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and*

      (b) *Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and*

   2. *Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;*

b. *Designate organizational personnel with system and information integrity responsibilities to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and*

c. *Review and update the current system and information integrity:*

   1. *Policy annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI; and*

   2. *Procedures annually and following any security incidents involving unauthorized access to CJI or systems used to process, store, or transmit CJI.*

SECTION 5.15

SI-2

SI-2 FLAW REMEDIATION

Control:

a. *Identify, report, and correct system flaws;*

b. *Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;*[5]

c. *Install security-relevant software and firmware updates within the number of days listed after the release of the updates;*[5]

- *Critical – 15 days*
- *High – 30 days*
- *Medium – 60 days*
- *Low – 90 days; and*

d. *Incorporate flaw remediation into the organizational configuration management process.*

SECTION 5.15

SI-7

(7) SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE[5]

Control:

Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

SECTION 5.15

SI-1, SI-2, SI-7

- SI-1, SI-2, and SI-7 are agency responsibilities.
- If an agency would like assistance with setting up best practice Policy and Procedure, Motorola can offer Cybersecurity Advisory Services. Motorola would be able to provide a security assessment of the agency's organizational environment and processes, including:
  - Consultative hours
  - Risk Assessment
  - Vulnerability Scanning
  - Penetration Testing

SECTION 5.15

SI-3

SI-3 MALICIOUS CODE PROTECTION

Control:

a. *Implement signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;*[5]

b. *Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;*

c. *Configure malicious code protection mechanisms to:*

   1. *Perform periodic scans of the system at least daily and real-time scans of files from external sources at network entry and exit points and on all servers and endpoint devices as the files are downloaded, opened, or executed in accordance with organizational policy; and*

   2. *Block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection; and*[5]

d. *Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.*[5]

SECTION 5.15

SI-4

SI-4 SYSTEM MONITORING[5]

Control:

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives:

a. Intrusion detection and prevention

b. Malicious code protection

c. Vulnerability scanning

d. Audit record monitoring

e. Network monitoring

f. Firewall monitoring;

and

2. Unauthorized local, network, and remote connections;

SECTION 5.15

SI-4

b. *Identify unauthorized use of the system through the following techniques and methods: event logging (ref. 5.4 Audit and Accountability);*

c. *Invoke internal monitoring capabilities or deploy monitoring devices:*

   1. *Strategically within the system to collect organization-determined essential information; and*

   2. *At ad hoc locations within the system to track specific types of transactions of interest to the organization;*

d. *Analyze detected events and anomalies;*

e. *Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;*

f. *Obtain legal opinion regarding system monitoring activities; and*

g. *Provide intrusion detection and prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring, and firewall monitoring software logs to organizational personnel with information security responsibilities weekly.*

Discussion: System monitoring includes external and internal monitoring. External

SECTION 5.15

SI-4

(2) SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS

Control:

Employ automated tools and mechanisms to support near real-time analysis of events.

Discussion: Automated tools and mechanisms include host-based, network-based, transport-based, or storage-based event monitoring tools and mechanisms or security information and event management (SIEM) technologies that provide real-time analysis of alerts and notifications generated by organizational systems. Automated monitoring techniques can

SECTION 5.15

SI-4

(4) SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC

Control:

a. *Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;*
b. *Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions such as: the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information.*

SECTION 5.15

SI-5

(5) SYSTEM MONITORING | SYSTEM-GENERATED ALERTS

Control:

Alert organizational personnel with system monitoring responsibilities when the following system-generated indications of compromise or potential compromise occur: inappropriate or unusual activities with security or privacy implications.

SECTION 5.15

SI-5

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control:

a. *Receive system security alerts, advisories, and directives from external source(s) (e.g., CISA, Multi-State Information Sharing & Analysis Center [MS-ISAC], U.S. Computer Emergency Readiness Team [USCERT], hardware/software providers, federal/state advisories, etc.) on an ongoing basis;*

b. *Generate internal security alerts, advisories, and directives as deemed necessary;*

c. *Disseminate security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and*

d. *Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.*

SECTION 5.15

SI-3, SI-4, & SI-5

- SI-3: Malicious Code Protection
- SI-4: System Monitoring
  - Automated Tools & Mechanisms for Real-Time Analysis
  - Inbound and Outbound Communications Traffic
  - System Generated Alerts
- SI-5: Security Alerts, Advisories, and Directives

PLAN FOR THE CJIS POLICY

SECTIONS 5.14 & 5.15

Internal Discussions

- Can your IT Dept consistently update critical patches in <15 days?
- Are your CJIS-broadcasting radios encrypted with >=128-bit encryption?
- Is your radio system being monitored in real-time?
- Does your radio, CAD, and data storage systems receive software patches, firmware updates, replacement parts, AND have maintenance contracts?
- Are your unique, specialized, proprietary systems with CJIS data like your LMR, CAD, and records being monitored 24x7 for malicious code, unauthorized access, and other CJIS-5.15 controls?
- Can your IT Dept detect unauthorized activity and malicious code on unique, specialized, proprietary systems like your LMR, CAD, and records?
- Are you concerned that your systems may be vulnerable to cyber attacks?

MOTOROLA SOLUTIONS CYBERSECURITY

TRUSTED CYBER PARTNER CAPABILITIES

ADVISORY

Assessment & Compliance

RISK ASSESSMENT

PENETRATION TESTING

MANAGED SECURITY

Vulnerability & Threat Insight

Detection & Response

CISO KPI Dashboard

Investigation & Reporting

Log Storage & Forensics

THREAT DETECTION & RESPONSE | **VULNERABILITY ASSESSMENT** | **PATCH TESTING & DEPLOYMENT**

24x7 Expert Security Operations Center

Public Safety Expertise and Deep Threat Intelligence

RECOVERY

Response & Recovery

INCIDENT RESPONSE PLANNING

INCIDENT RECOVERY

CYBERSECURITY TRAINING

PUBLIC SAFETY THREAT ALLIANCE

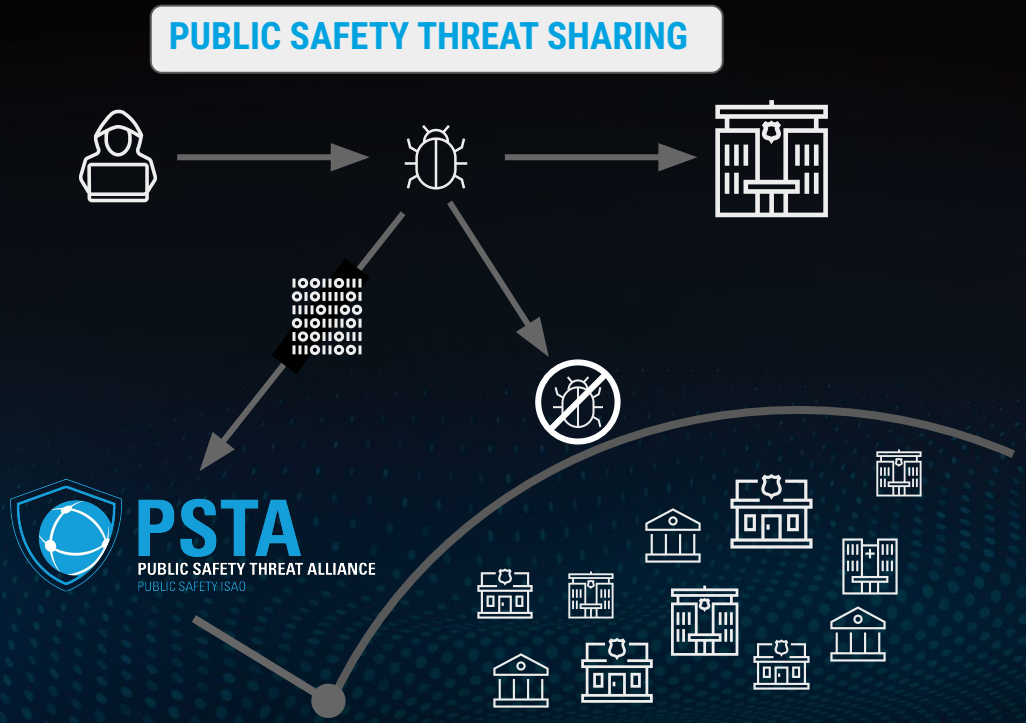
CISA-Registered ISAO

Membership in the Public Safety Threat Alliance (PSTA) is open to all public safety agencies at **no cost**

- Secure Portal for Information Sharing
- Vulnerability & Threat Advisories
- Bi-weekly, Monthly, and Quarterly Reports
- Quarterly Webinars
- Monthly Analyst Calls

INCREASE IN ATTACKS

2019		2022
154 ATTACKS	→	225 ATTACKS



MOTOROLASOLUTIONS.COM/PSTA

ADOPT A HOLISTIC SOLUTION FOR CYBERSECURITY

Have a Plan

1. **KNOW YOUR NETWORK** - *Hardware, Software, Applications, Data Flows*
2. **KNOW YOUR ADVERSARY** - *Who is attacking you and how might they do it?*
3. **PATCH, ASSESS, MONITOR** - *Blocking and tackling*
4. **KNOW WHAT NORMAL LOOKS LIKE** - *The only way to detect abnormal*
5. **EDUCATE YOUR USERS** - *Cybersecurity is everyone's responsibility*
6. **KNOW HOW TO RESPOND TO A CYBER ATTACK** - *Train Hard, Fight Easy*

FUNDING

SLCGP

State & Local Cybersecurity Grant Program

OBJECTIVE 4 – FUNDING

State and Local Cybersecurity Grant Program (SLCGP)

The SLCGP addresses cybersecurity risks and threats to critical infrastructure information systems owned or operated by, or on behalf of, state, local and territorial governments.

The program, which is jointly managed by the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Emergency Management Agency (FEMA), provides a total of $1 billion over four years in dedicated funding for state and local cybersecurity. For more information about the SLCGP, contact your Motorola Solutions Representative.

SLCGP is an ongoing grant award to states. The SLCGP began awarding grants during the same month that the CJIS Policy 5.9.2 was published (December 2022).

The SLCGP can be used for cybersecurity upgrades, including CJIS 5.9.2 Policy.

MOTOROLA SOLUTIONS

THANK YOU
QUESTIONS?

LINKS

Criminal Justice Information Services (CJIS) Security Policy (External)